5M

УДК 004.89

Н.А. Маслова, В.В. Шамаев
КП «Компания "Вода Донбасса"», Украина
Донецкий национальный технический университет, г. Донецк, Украина
masgpp@list.ru, shamaev@dgtu.donetsk.ua

Принципы адаптации в защите корпоративных систем

В работе систематизированы основные принципы адаптации, используемые в системах защиты информации, приведена методология построения систем защиты на основе адаптивного подхода, предложена методика оценки эффективности адаптивной системы защиты. Приведены примеры включения интеллектуальных адаптивных систем защиты в корпоративное управление.

Введение

Современные компьютерные системы и сети находятся в состоянии постоянного развития и модификации, а объемы анализируемых данных в мире удваиваются каждый год. Поэтому для обеспечения требуемого уровня защиты информации необходимо гибко и оперативно реагировать на изменяющиеся условия, обеспечивать надежную защиту с учетом постоянного изменения входных воздействий, предупреждать действия злоумышленников, т.е. иметь адаптивную и саморазвивающуюся систему защиты информации (СЗИ).

Целью данной работы является исследование особенностей применения адаптивных алгоритмов при построении саморазвивающихся систем защиты информации в корпоративных сетях и разработка методики оценки эффективности защиты адаптивной модели.

Основные принципы адаптации в системах защиты информации

Термин «адаптация» в компьютерных информационных системах подразумевает процесс целенаправленного изменения структуры, алгоритма или параметров системы с целью повышения эффективности её функционирования. Адаптивная система является системой с обратной связью, классификация адаптивности которой проводится по трем основным признакам:

– уровню адаптации (структурная, алгоритмическая, параметрическая);

– механизму адаптации (с эталонной моделью; аналитически-настраиваемая система; экстремальная система);

– способу адаптации (с дискретной или непрерывной настройкой).

Основные требования к адаптивным алгоритмам в системах защиты информации:

– оперативность во времени, что связано с необходимостью применения эффективных по быстродействию алгоритмов;

– наиболее низкий из допустимых уровень сложности контура адаптации;

– автоматический или автоматизированный характер процедуры адаптации;

– минимальное число управляемых параметров, что позволит минимизировать затраты времени и памяти, необходимые для реализации алгоритма, но обеспечить заданный уровень защиты.

Использование аддитивного подхода позволяет контролировать, обнаруживать и реагировать в реальном режиме времени на риски безопасности, используя правильно спроектированные и хорошо управляемые процессы и средства.

В целом аддитивный процесс защиты должен включать:

- технологию анализа защищенности или поиска уязвимостей;
- методы обнаружения атак;
- адаптивный механизм, объединяющий и расширяющий предыдущие пункты;
- управляющий компонент.

Особенностью адаптивных систем защиты является наличие специальных алгоритмов, которые обеспечивают решение ряда взаимосвязанных задач, таких, как сбор и анализ информации о состоянии компьютерной системы; оценка состояния внешней среды; принятие решения о необходимости применения мер защиты; выбор управляющих параметров; синтез схемы адаптации и реализацию механизмов её реализации; определение эффективности системы защиты [1].

Средства обеспечения безопасной работы систем защиты корпоративной информации

Особенностью систем защиты информации в корпоративных системах является комбинация как минимум трех проблем: защита информации в компьютерных сетях; обеспечение безопасности баз данных; обеспечение безопасной работы систем автоматической обработки информации [2].

Защита баз данных является одной из самых сложных задач систем защиты информации в корпоративных системах. Наиболее распространенными угрозами, характерными для баз данных, являются хищения, утрата, уничтожение, модификация данных и отказ от подлинности. Основными механизмами обеспечения безопасности баз данных являются шифрование; контроль доступа; мониторинг и аудит.

К традиционным средствам обеспечения информационной безопасности (ИБ) корпоративных компьютерных сетей относят антивирусы, детекторы уязвимостей, межсетевые экраны и детекторы вторжений. Они решают отдельные задачи обеспечения ИБ корпоративной сети и, как правило, могут быть преодолены при командной работе квалифицированной группы нарушителей.

К средствам обеспечения безопасной работы систем обработки информации относятся механизмы предотвращения вторжений, авторизация, разграничение прав доступа, криптозащита (носителей информации, сетей, парольная защита), управление полномочиями пользователей. С целью контроля состояния системы используют базы сигнатур известных атак, а в качестве основных источников информации – системные журналы и файлы, анализируют содержимое сетевого трафика и файлов. Блоки СЗИ для обеспечения безопасной работы систем автоматической обработки информации размещаются обычно на локальных серверах и сетевых узлах распределенных систем. При этом нейтрализуются известные угрозы безопасности системы, однако при расширении поля угроз, наличии комбинированных компьютерных атак традиционные системы уязвимы.

Сегодня администратору безопасности уже недостаточно иметь средства управления учетными записями и ресурсами, либо механизмы защиты от какой-то конкретной угрозы. Ему необходим механизм прослеживания тенденций и прогнозирования событий в области безопасности. Такие механизмы разработаны для контроля уязвимостей, обнаружения атак, для систем сетевого и системного мониторинга, однако комплексной системы, которая охватывала бы все аспекты, необходимые для защиты корпоративных систем, до настоящего времени не разработано.

Поэтому решение проблем безопасности корпоративных информационных систем требует дальнейшего поиска эффективных механизмов. Они должны работать в режиме реального времени, обладать высокой чувствительностью к изменениям в информационной инфраструктуре, включать базу знаний, накопленную в процессе работы, содержать элементы интеллектуального анализа данных и быть способными сгенерировать решение в соответствии с заданной целевой функцией в постоянно изменяющихся условиях внешней среды.

Предпосылками использования интеллектуальных алгоритмов в защите корпоративных систем являются клиент-серверная технология, распределенные базы данных, наличие хранилищ информации, применение современных сетевых технологий и разнообразного инструментария, используемого для сбора, обработки, визуализации и анализа данных.

Необходимость использования инструментария интеллектуального анализа данных (ИАД) в СЗИ корпоративных систем проистекает из разнородности структур информационных пространств этих систем; сложности получения аналитической информации из больших баз данных; значительного числа пользователей, одновременно работающих в системе; требований постоянного контроля и принятия оперативных и обоснованных управленческих решений, зависящих от множества факторов.

К часто используемым в компьютерных сетях интеллектуальным средствам относят базы знаний в составе экспертных систем, системы на основе байесовского метода, нечеткие логические системы, нейронные сети, эволюционные методы и гибридные интеллектуальные системы. Основными задачами, решаемыми интеллектуальными средствами обеспечения информационной безопасности компьютерной сети, являются классификация и кластеризация.

Методология построения системы защиты информации с применением ИАД

Выделяют два подхода к построению систем защиты информации с применением ИАД – традиционный, в качестве инструментария использующий нейросетевые технологии, системы нечеткой логики или экспертные системы, и эволюционный, использующий адаптивные алгоритмы.

При традиционном подходе к построению системы защиты с применением инструментария ИАД используются искусственные нейронные сети, деревья решений и алгоритмы классификации, методы нечеткой кластеризации, ассоциативные правила, алгоритмы ограниченного перебора, кластерный анализ.

Нейронные сети используются для контроля трафика защищаемой локальной сети, поиска скрытых закономерностей в массивах первичных данных, выявления вторжений. Для предсказания значения целевого показателя используются наборы входных переменных, математических функций активации и весовых коэффициентов входных параметров. Выполняется итеративный обучающий цикл, нейронная сеть модифицирует весовые коэффициенты до тех пор, пока предсказываемый выходной параметр соответствует действительному значению. После обучения нейронная сеть становится моделью, которая применяется при прогнозировании.

Механизмы классификации используются на первоначальном уровне, например, для систематизации способов защиты (нечеткие заключения) по вектору нечетких признаков угроз. Если достоверность классификации по известным угрозам меньше некоторого уровня, то при наличии признаков атаки классификация расширяется за счет введения новой градации в классификацию – решается задача кластеризации угроз. Ассоциации выявляют причинно-следственные связи и определяют вероятности или коэффициенты достоверности, позволяя делать соответствующие выводы. Модель

Деннинга содержит набор профилей для легальных пользователей, сравнивает текущие действия с соответствующим профилем, обновляет профиль и сообщает о любых обнаруженных аномалиях.

Недостатками традиционного подхода являются:

1) базы знаний формируются экспертами, т.е. принцип включения в них ситуаций субъективен;

2) базы знаний необходимо периодически обновлять, упорядочивать, систематизировать, что является трудоемкой и дорогостоящей процедурой;

3) при традиционном подходе существует задержка во времени между появлением новой атаки и средств защиты от нее (запаздывающее противодействие);

4) атаки постоянно видоизменяются, совершенствуются, «маскируются» под стандартные процедуры, что требует постоянного совершенствования, усложнения средств защиты.

С учетом вышесказанного, проблема эволюционного развития систем информационной безопасности, предполагающая использование адаптивных алгоритмов и направленная на защиту корпоративных систем, актуальна.

Построение модели интеллектуального анализа данных является частью масштабного процесса, в который входят все задачи, от формулировки вопросов выбора и хранения данных и создания модели до развертывания модели в рабочей среде. Для построения модели используют математические основы скрытых Марковских цепей, интеллектуальные мультиагентные технологии, аппарат нечетких множеств и семиотического моделирования и т.д. Однако главным требованием при этом является комплексный, системный подход, единый процесс построения адаптивной системы с учетом требований и методологии защиты информации.

Этапами построения адаптивной саморазвивающейся системы, построенной с применением элементов ИАД, являются следующие моменты [3].

1. Составление перечня основных источников данных и выбор информации, подлежащей анализу.

2. Постановки задачи (анализ требований, определение проблем для решения, метрик, по которым выполняется оценка модели, определяются задачи для проекта интеллектуального анализа данных).

3. Сортировка и очистка данных (упорядочение, удаление недопустимых и ошибочных комбинаций, согласование данных).

4. Формирование матриц адаптируемых экспертных оценок и на их основе создание исходных систем нечетких правил и классификаторов.

5. Классификация регистрируемых событий (например, угроз по вектору признаков атак и механизмов защиты по вектору угроз, выделение кластеров, упрощающих разделение данных на обучающий и проверочный наборы).

6. Предварительный статистический анализ, получение контрольных метрик и закономерностей. Создание структуры интеллектуального анализа данных.

7. Составление систем нечетких правил, которые реализуются в виде специализированных структур, подбор классификаторов, формирование признака структуры (происходит постоянно и независимо от дальнейшей работы алгоритма).

8. Построение модели.

9. Передача опыта адаптивной СЗИ (наследование) по обеспечению информационной безопасности.

10. Обучение классификаторов на обучающей выборке – подмножеству входных векторов, формирование информационных полей четких классификаторов.

11. Адаптация системы к реальным условиям.

12. Коррекция матриц первоначальных оценок и систем нечетких правил по результатам адаптации.

13. Формулирование новых нечетких правил в случае расширения классификации, разработка спецификации на создание нового механизма защиты. Формирование комплекса оценок защищенности системы.

14. Анализ структуры классификаторов и выявление недостатков в системе защиты, оценка эффективности системы, включение в нее дополнительных механизмов защиты.

15. Контроль целостности данных и программных модулей, при необходимости – восстановление программной среды, изменение структуры системы информационной безопасности.

Порядок действий согласно методу проектирования адаптивных СЗИ может изменяться, но обязательными являются [4]:

1) формирование многомерных матриц адаптируемых оценок и на их основе создание исходных систем нечетких правил и классификаторов (на нижних уровнях защиты – классификаторов «признаки атаки – угрозы», на верхних уровнях защиты – классификаторов «угрозы – механизмы защиты»);

2) идентификация выявленной угрозы и при расширении поля известных угроз – кластеризация угроз с последующей адаптацией информационных полей путем обучения алгоритма ИАД;

3) коррекция и расширение системы нечетких правил, вызванная изменением поля угроз;

4) модификация систем нечетких правил и матриц экспертных оценок в результате обучения классификаторов уровней защиты;

5) описание нового механизма защиты;

6) формулировка спецификации на создание нового механизма защиты;

7) анализ защищенности ИТ-системы (в случае экономической целесообразности) включает новый механизм защиты в состав защиты.

Метод оценки эффективности адаптивных систем защиты информации

Эффективность функционирования СЗИ зависит от множества действующих взаимосвязанных между собой элементов и, как правило, оценивается совокупностью критериев, находящихся в сложных конфликтных взаимоотношениях.

Отсутствие на сегодняшний день общего подхода к решению задач данного класса закономерно влечет за собой многообразие различных не взаимосвязанных методов оценки качества.

Простейшей схемой построения защиты, устраняющей 20 – 30% угроз, является схема Безопасность = Традиционные средства защиты.

Более надежной схемой построения защиты, по данным «Компьютер-Пресс», обеспечивающей 40 – 60% эффективность, является комплексный подход, наличие четко сформулированных и действующих политик безопасности, использование разветвленного перечня традиционных средств защиты, постоянный контроль ситуации и безотлагательное применение мер защиты. При этом схема защиты выглядит следующим образом: Безопасность = Политика безопасности + Традиционные средства защиты + Анализ риска + Реализация контрмер.

И, наконец, модель адаптивного управления безопасностью тот же источник предлагает описывать формулой Безопасность = Анализ риска + Политика безопасности + Традиционные средства защиты + Реализация контрмер + Аудит + Мониторинг + Реагирование.

Процесс определения эффективности систем защиты начинают с выбора и обоснования показателей (критериев) оценки эффективности системы защиты, а затем переходят

к подбору или разработке методик расчета этих показателей. В [5] приведен перечень распространенных подходов к выбору критериев и оценке параметров, показатели эффективности систем защиты и методики их расчета.

Наиболее распространенным способом оценки эффективности СЗИ является оптимизационный или комбинаторный подход. При этом решается задача оптимизации вида: максимизировать некую функцию при заданных ограничениях. В случае адаптивных систем указанную методику предлагается расширить параметром k, характеризующим этапы адаптивного процесса.

Введем нижеследующие обозначения:

$U = \{u_j\}$ – множество угроз безопасности, $j = 1, \dots m$;

$A^k = \{a^k_i\}$ – множество механизмов безопасности, используемых на k-м этапе адаптивного процесса,

$X = \{x_i\}$ – множество требований безопасности,

$i = 1\dots n$, $k = 0...R$.

$C^k = \{c^k_i\}$ – допустимые затраты на создание защиты (объем затрат на сопровождение системы с учетом реализации k-го этапа адаптивного процесса), причем c^1_i – это затраты на начальную разработку, обучение и первоначальный запуск адаптивной системы;

$d^k(i, j)$ – эффективность нейтрализации i-м механизмом безопасности j-й угрозы на k-м этапе.

Для построения математической модели вводят переменную $p(i,j)$, равную 1, если j-я угроза устраняется с помощью i-го механизма, и нулю – в противном случае и q, такую, что

$$q(i,j)=\begin{cases}1-\textit{если } i-\textit{й механизм безопасности используется для устранения } j-\textit{й угрозы};\\ 0-\textit{в противном случае}\end{cases}$$

Если информационные угрозы между собой не связаны, то требуется найти максимальный эффект от нейтрализации множества информационных угроз U с помощью задекларированных в системе средств защиты A при ограничениях на общий объем затрат C.

$$\sum_{k=1}^{r}\ \sum_{j=1}^{m}\sum_{i=1}^{n} d^k(i,j)\,p(i,j) \Rightarrow \max \tag{1}$$

при ограничениях

$$\sum_{i=1}^{n} c(i) * sign \sum_{uj\in U}^{n} p(i,j) \le C \tag{2}$$

$$p(i,j)\in(1,0),\ j = 1\dots m;\ i = 1\dots n. \tag{3}$$

Несколько видоизменив постановку задачи и введя понятие функции принадлежности $\mu^A(x_i)$ в соответствии с [6], получим вариант оценки эффективности информационной системы защиты в случае нечётких показателей. Пусть W – счётное множество показателей $W = \{w_i\}$, $i = 1...n$, n – количество показателей. Принадлежность к определённому уровню безопасности определяем на заданном промежутке, например, $[0, T]$. Тогда множество значений V, определяющих выполнение требований безопасности, определяется как: $V = \sum_{i=1}^{n} \frac{\mu^A(x_i)}{x_i}$, где $\frac{\mu^A(x_i)}{x_i}$ – пара «функция принадлежности \ элемент».

При этом, если, например, $X = \{1, 2, 3, 4, 5\}$ – заданные наборы требований защиты системы, тогда нечёткое множество оценки защищённости системы, имеющей определённые критерии безопасности, будет: А = 0,2/1 + 0,4/2 + 0,6/3 + 0,8/4 + 1/5.

Интерпретация указанного приведена в табл. 1.

Таблица 1

i	Требование безопасности	Состояние безопасности системы
1	1	абсолютно незащищённая
2	2	недостаточно защищённая
3	3	защищённая
4	4	достаточно защищённая
5	5	абсолютно защищённая

Разные состояния безопасности системы выделяются в виде подмножеств нечёткого множества, а вероятность взлома оцениваемой системы может соответствовать кардинальному числу (мощности) нечёткого множества.

При таком подходе для оценки эффективности защищённости адаптивной системы защиты необходимы данные о необходимых требованиях защищённости и данные о полноте выполнения этих требований.

Подобный подход позволяет добиться постоянного мониторинга состояния информационной безопасности системы, выполнить прогноз возможности осуществления атак, провести изменение требований к переменным безопасности. Получаем возможность контроля вновь возникающих угроз, устранять уязвимости, которые могут привести к реализации угрозы, анализировать условия, приводящие к появлению уязвимостей.

Применение эффективных алгоритмов

Построение адаптивных саморазвивающихся систем защиты невозможно без быстродействующих алгоритмов. Например, одним из недостатков традиционного подхода является задержка во времени между появлением новой атаки и средств защиты от нее. В теории СЗИ различают одновременное, опережающее и запаздывающее противодействие. Идеальным вариантом является опережающее противодействие, а для этого необходимо не только наличие методик, позволяющих своевременно обнаружить угрозу безопасности системе, но и применение алгоритмов, способных выполнить анализ ситуации и своевременно ликвидировать результаты вторжения.

Важным моментом является использование в адаптивных блоках алгоритмов сортировки, которые оцениваются по скорости выполнения и эффективности использования памяти. Если алгоритм сортировки использует только абстрактную операцию сравнения ключей, то его вычислительная сложность $O(n \log n)$ операций сравнения. При параллельном вычислении n ситуаций можно отсортировать за $O(\log^2 n)$ операций, а худшими являются алгоритмы сортировки, вычислительная сложность которых $O(n^2)$ операций. Требуемый объем памяти для реализации алгоритмов сортировки, как правило, составляет $O(\log n)$ ячеек.

Методы сортировки, рекомендуемые для использования в системе – сортировка вставками (может сортировать список по мере его получения), блочная сортировка (относится к классу быстрых алгоритмов с линейным временем исполнения $O(N)$).

Задача классификации – одна из наиболее распространенных задач в анализе данных. На сегодняшний день разработано большое число подходов к решению задач классификации, использующих такие алгоритмы, как деревья решений, нейронные сети, логистическая регрессия, метод опорных векторов, дискриминантный анализ, ассоциативные правила. Одним из эффективных алгоритмов классификации является так называемый «наивный» (упрощенный) алгоритм Байеса. С точки зрения быстроты обучения, стабильности на различных данных и простоты реализации, алгоритм Байеса превосходит практически все известные эффективные алгоритмы классификации. Обуче-

ние алгоритма производится путем определения относительных частот значений всех атрибутов входных данных при фиксированных значениях атрибутов класса. Классификация осуществляется путем применения правила Байеса для вычисления условной вероятности каждого класса для вектора входных атрибутов. Входной вектор приписывается классу, условная вероятность которого при данном значении входных атрибутов максимальна. Алгоритм строится в предположении, что входные атрибуты условно (для каждого значения класса) независимы друг от друга [6].

Примеры применения адаптивного подхода в защите корпоративных систем

Подтверждением распространения адаптивных систем в корпоративном управлении являются следующие примеры.

Microsoft SQL Server 2008 предоставляет интегрированную среду для создания моделей интеллектуального анализа данных и работы с ними. Эта среда называется Microsoft SQL Server Analysis Services и состоит из набора специальных инструментов (Business Intelligence Development Studio, SQL Server Management Studio, Microsoft SQL Server 2008 Integration Services, BI Development Studio).

Данная среда включает алгоритмы интеллектуального анализа данных и средства, облегчающие разработку комплексного решения, применимого в рамках самых разных проектов. Так, например, Microsoft заявляют о применении «технологии активной защиты», основанной на оценке поведения программ с точки зрения их потенциальной опасности. В частности, СЗИ корректируют средства защиты компьютера при изменении его статуса или блокируют его, если возникает подозрение в заражении вирусом или проникновении злоумышленника.

В апреле 2010 года фирма IBM представила системы интеллектуального анализа и обработки транзакций, помогающие извлекать важные знания из огромных массивов данных, в том числе и определения скрытых возможностей или выполнения анализа систем на поведенческом уровне (http://www.ibm.com/news).

Компания ISS (Internet Security Systems) разработала модель адаптивного управления безопасностью, получившую название ANS (Adaptive Network Security). *Адаптивный компонент* ANS позволяет модифицировать процесс анализа защищенности, предоставляя самую последнюю информацию о новых уязвимостях. Он также модифицирует компонент обнаружения атак, дополняя его последней информацией о подозрительных действиях и атаках.

Семейство продуктов SAFEsuite, разработанное ISS, Inc., в настоящий момент является наиболее мощным комплексом систем, включающим в себя такие компоненты модели адаптивного управления безопасностью сети, как: систему анализа защищенности на уровне сети Internet Scanner; системы анализа защищенности на уровне операционной системы и прикладного ПО System Scanner и Online Scanner; систему анализа защищенности на уровне СУБД Database Scanner; системы обнаружения атак RealSecure (Network Sensor, Appliance, OS Sensor, Server Sensor); систему поддержки принятия решения и прогнозирования в области безопасности SAFEsuite Decisions.

Российская компания «Информзащита» сообщает о разработке концепции и реализации подсистемы адаптивной безопасности и противодействия внешним атакам ОАО «Вымпелком» (http://www.infosec.ru).

Примером адаптивного компонента может служить механизм обновления баз данных антивирусных программ, которые являются частным случаем систем обнаружения атак.

Однако эффективно реализовать все описанные технологии в одной системе пока не удается, поэтому пользователям приходится применять совокупность систем защиты, объединенных единой концепцией безопасности и продолжать поиски лучших с точки зрения соотношения «эффективность – затраты» решений.

Выводы

Адаптивные алгоритмы являются необходимым и современным дополнением такой крупной информационной структуры, как корпоративная система. Одной из её составных частей является система защиты информации. Средства защиты должны постоянно совершенствоваться и развиваться, ввиду чего построение адаптивной саморазвивающейся СЗИ является актуальным, а использование наряду с ИАД быстрых алгоритмов увеличит эффективность системы.

В работе изложены основные принципы адаптации, применимые в системах защиты информации, предложена модель адаптивной системы защиты информации, отличающаяся использованием механизмов интеллектуального анализа данных.

Описаны методы оценки эффективности адаптивной системы защиты информации, отмечена необходимость использования эффективных алгоритмов на различных этапах работы адаптивной системы защиты.

Приведенные в последней части статьи данные свидетельствуют об актуальности рассматриваемой темы, сложности и необходимости развития адаптивного подхода к решению проблемы защиты больших систем. И, разумеется, практическая ценность развития этого направления подтверждается востребованностью подобных алгоритмов на рынке ИТ-технологий.

Литература

1. Щербаков А.Ю. Компьютерная безопасность. Теория и практика / Щербаков А.Ю. – М. : Нолидж, 2001. – 352 с.
2. Шаньгин В.Ф. Защита информации в распределенных корпоративных сетях и системах / В.Ф. Шаньгин, А.В. Соколов. – Изд-во : ДМК, 2002. – 134 с.
3. Маслова Н.А. О применении интеллектуального анализа данных для защиты информации корпоративных систем / Н.А. Маслова // Штучний інтелект. – 2009. – № 4. – С. 66-74.
4. Нестерук Ф.Г. Основы организации адаптивных систем защиты информации : [учебное пособие] / Нестерук Ф.Г., Нестерук Г.Ф., Осовецкий Л.Г. – СПб. : СПбГУ ИТМО, 2008. – 112 с.
5. Маслова Н.А. Методы оценки эффективности систем защиты информационных систем / Н.А. Маслова // Штучний інтелект. – 2008. – № 4. – С. 253-264.
6. Домарев В.В. Безопасность информационных технологий. Методология создания систем защиты / Домарев В.В. – К. : ООО «ТИД «ДС», 2002. – 688 с.

Н.О. Маслова, В.В. Шамаєв

Принципи адаптації у захисті корпоративних систем
У роботі систематизовані основні принципи адаптації, які використовуються в системах захисту інформації, наведена методологія побудови систем захисту на основі адаптивного підходу, запропонована методика оцінки ефективності адаптивної системи захисту. Наведені приклади включення інтелектуальних адаптивних систем захисту в корпоративне управління.

N.A. Maslova, V.V. Shamayev

Principles of Adaptation in Corporate Security Systems
The basic principles of adaptation, which are used in the security systems of information are systematized, methodology of construction of the security systems on the basis of adaptive approach is described, the method of estimation of efficiency of adaptive security systems is offered in the article. The examples of the intellectual adaptive security systems which are included in a corporate management are described.

Статья поступила в редакцию 01.06.2010.